CAPSTONE PROJECT

NETWORK INTRUSION DETECTION

Presented By : Shaik Afrin
College Name : St.Ann’s College Of Engineering & Technology (Chirala)
Department : Computer Science & Engineering

edunet foundation

OUTLINE

- Problem Statement
- Proposed System/Solution
- System Development Approach
- Algorithm & Deployment
- Result (Output Image)
- Conclusion
- Future Scope
- References

PROBLEM STATEMENT

Network Intrusion Detection

Create a robust network intrusion detection system (NIDS) using machine learning. The system should be capable of analyzing network traffic data to identify and classify various types of cyber-attacks (e.g., DoS, Probe, R2L, U2R) and distinguish them from normal network activity. The goal is to build a model that can effectively secure communication networks by providing an early warning of malicious activities.

PROPOSED SOLUTION

- The proposed system aims to address the challenge of predicting the Network Intrusion Detection. This involves leveraging data analytics and machine learning techniques to learn and predict Network Intrusion accurately. The solution will consist of the following components:
- Data Collection:
  - Gather historical data on network intrusions, including protocol type, services and other relevant factors.
- Data Preprocessing:
  - Clean and preprocess the collected data to handle missing values, outliers, and inconsistencies.
  - Feature engineering to extract relevant features from the data that might impact Network Intrusion prediction.
- Machine Learning Algorithm:
  - Implement a machine learning algorithm, particularly classification algorithm, to predict Network Intrusion based on historical patterns.
- Deployment:
  - Develop a user-friendly interface or application that provides real-time predictions for Network Intrusion.
  - Deploy the solution on a scalable and reliable platform, considering factors like server infrastructure, response time, and user accessibility.
- Evaluation:
  - Assess the model's performance using appropriate metrics such as Precision, Recall, F1-score, Accuracy Score and other relevant metrics.
  - Fine-tune the model based on feedback and continuous monitoring of prediction accuracy.
  - Result

SYSTEM APPROACH

We are training our model on Decision Tree classifier using ensemble learning method across various pipelines and we will choose the one with highest accuracy on test data.

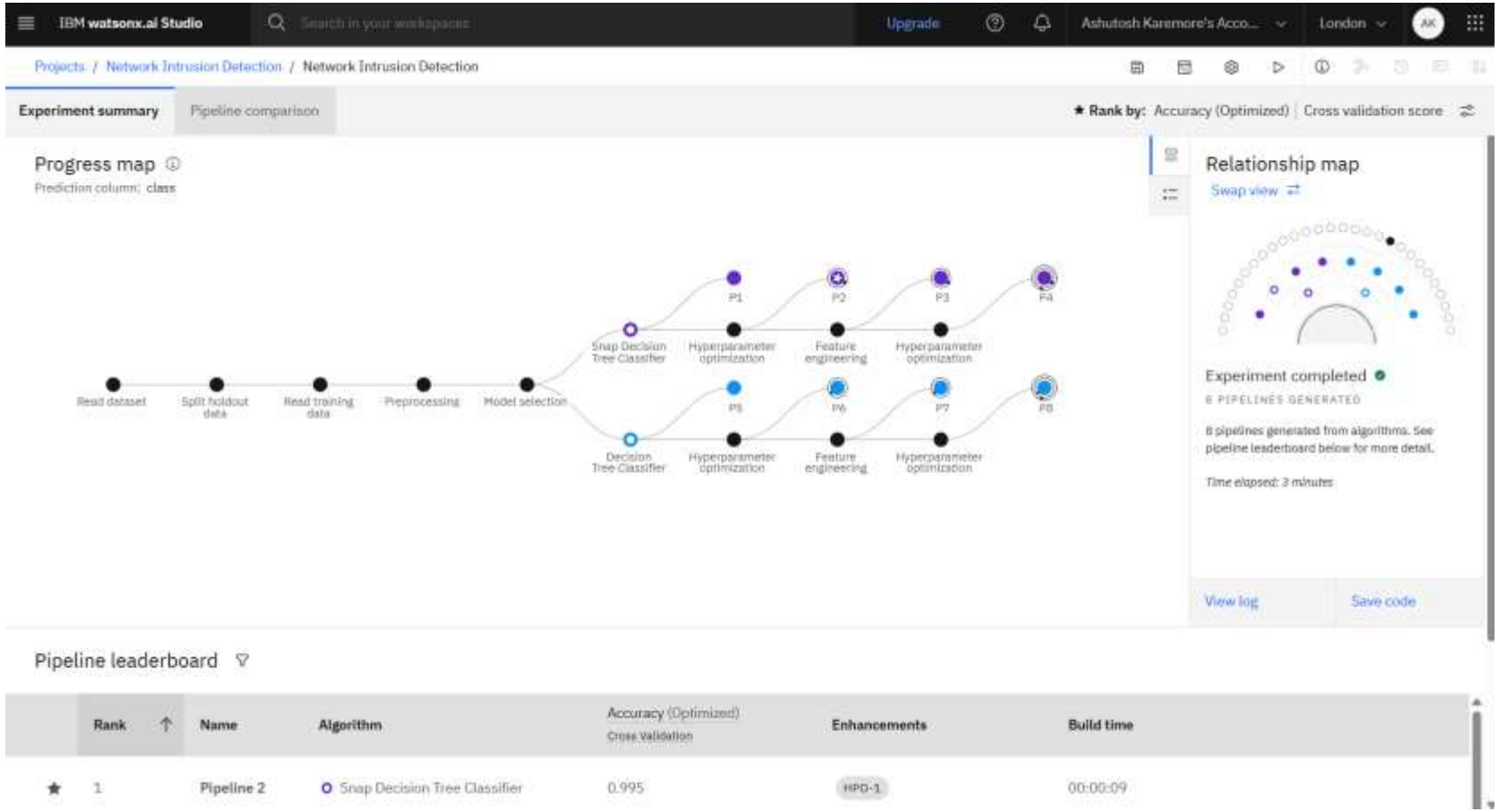
Decision Tree is a tree-based machine learning algorithm which has upside down tree-like structure consisting of different decision nodes created from features with low impurity at each depth. The split is decided based on feature value.

ALGORITHM & DEPLOYMENT

- In the Algorithm section, describe the machine learning algorithm chosen for predicting network intrusion.
- Algorithm Selection:
  - We are training our model on Decision Tree classifier using ensemble learning method across various pipelines and we will choose the one with highest accuracy on test data.
  - Decision Tree is a tree-based machine learning algorithm which has upside down tree-like structure consisting of different decision nodes created from features with low impurity at each depth. The split is decided based on feature value.
- Data Input:
  - Input features are selected by the algorithm based on rate of impurity measured by Gini Impurity or Entropy Value, the feature with low impurity and high information gain is selected as a decision node till a leaf node is found which has zero impurity.
- Training Process:
  - Training is done on IBM cloud ML services platform which leverages ensemble techniques and uses the best model based on cross-validation score.
- Prediction Process:
  - Predictions are made by the model based on the features values provided by the user, the model outputs class 1 or 0 for Intrusion or not an intrusion

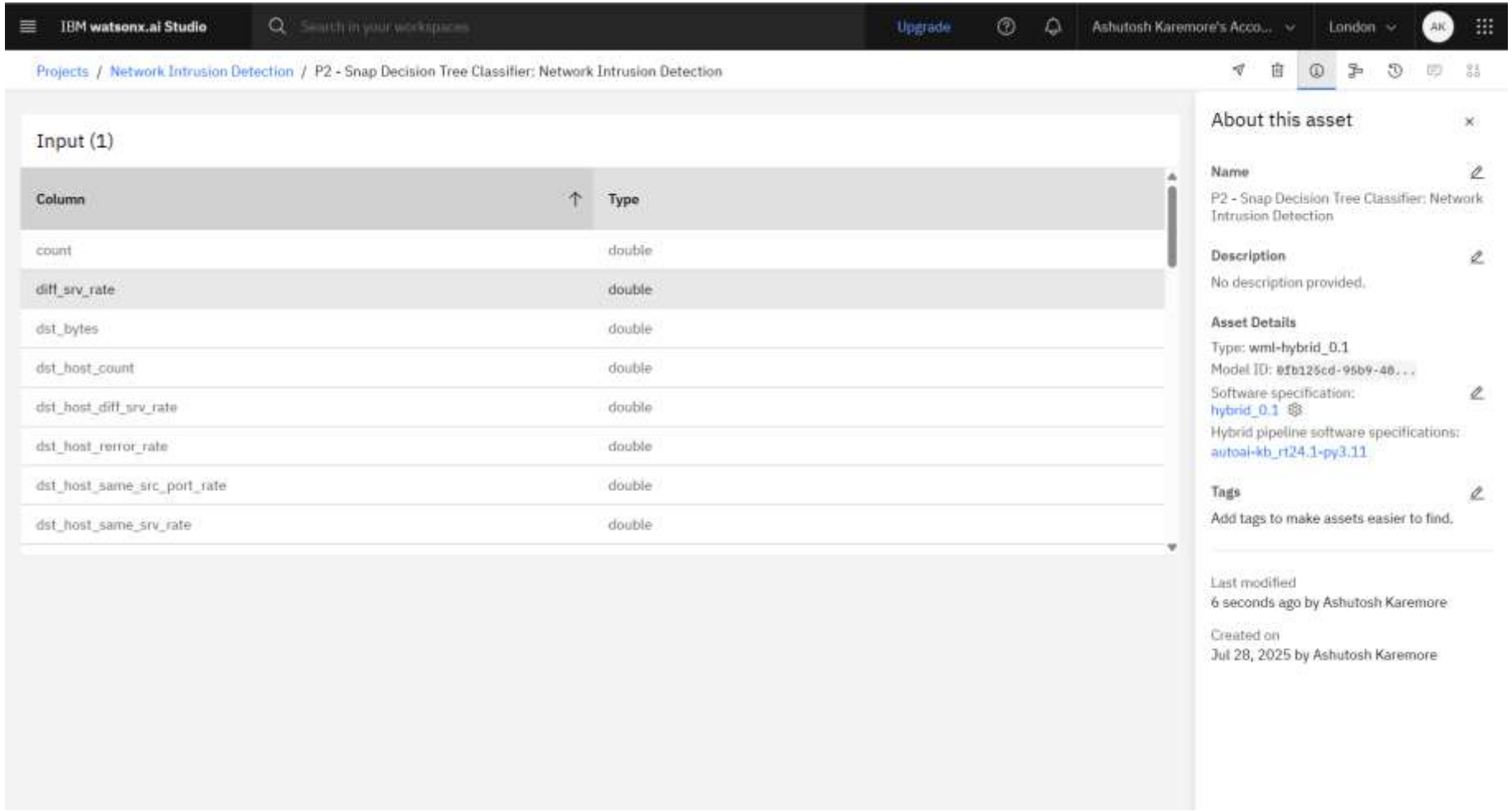
RESULT

Link to deployed model : https://eu-gb.ml.cloud.ibm.com/ml/v4/deployments/a1eeb2e4-9788-473d-953c-bce56dc707c1/predictions?version=2021-05-01



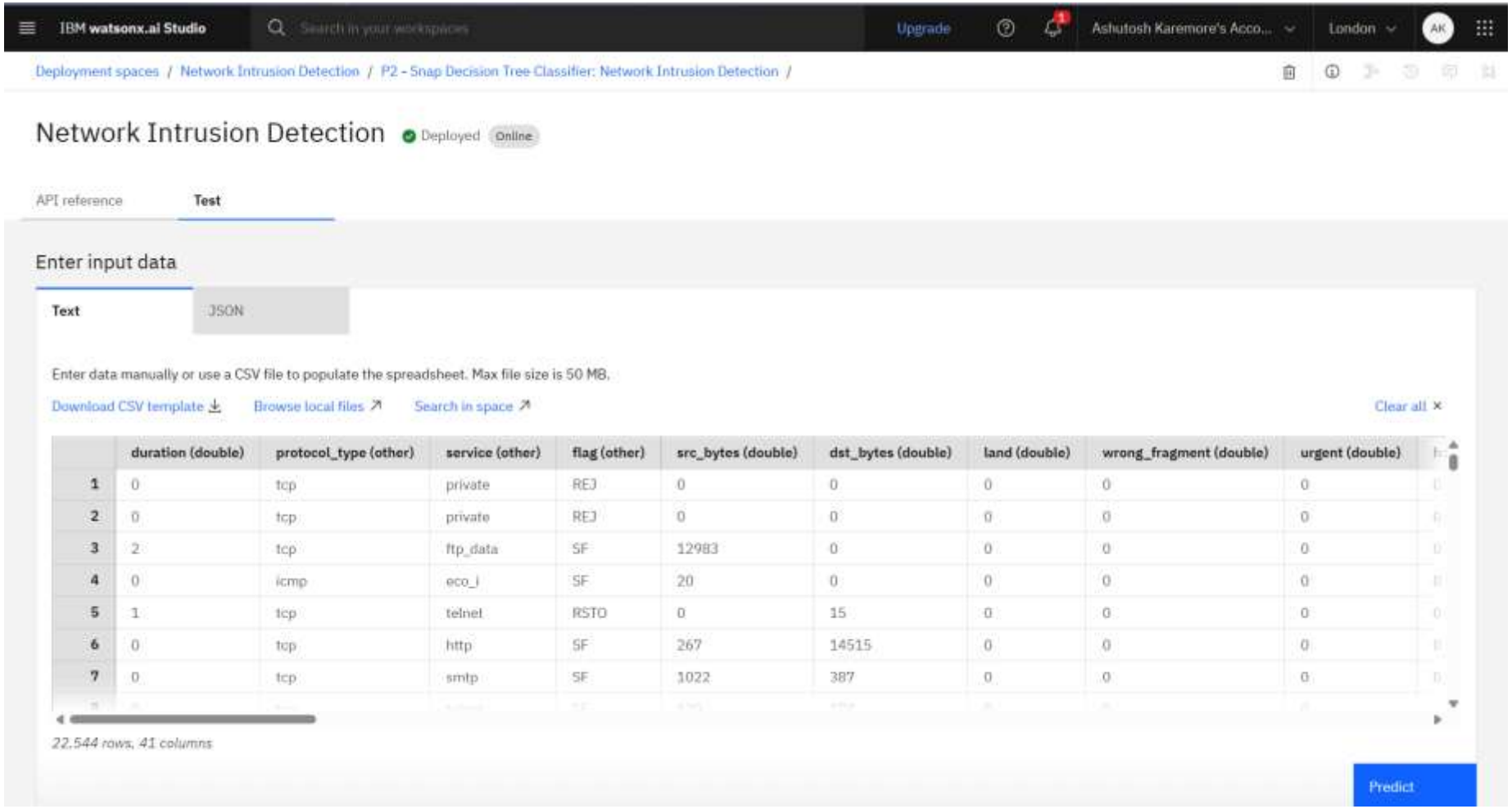
edunet foundation

RESULT



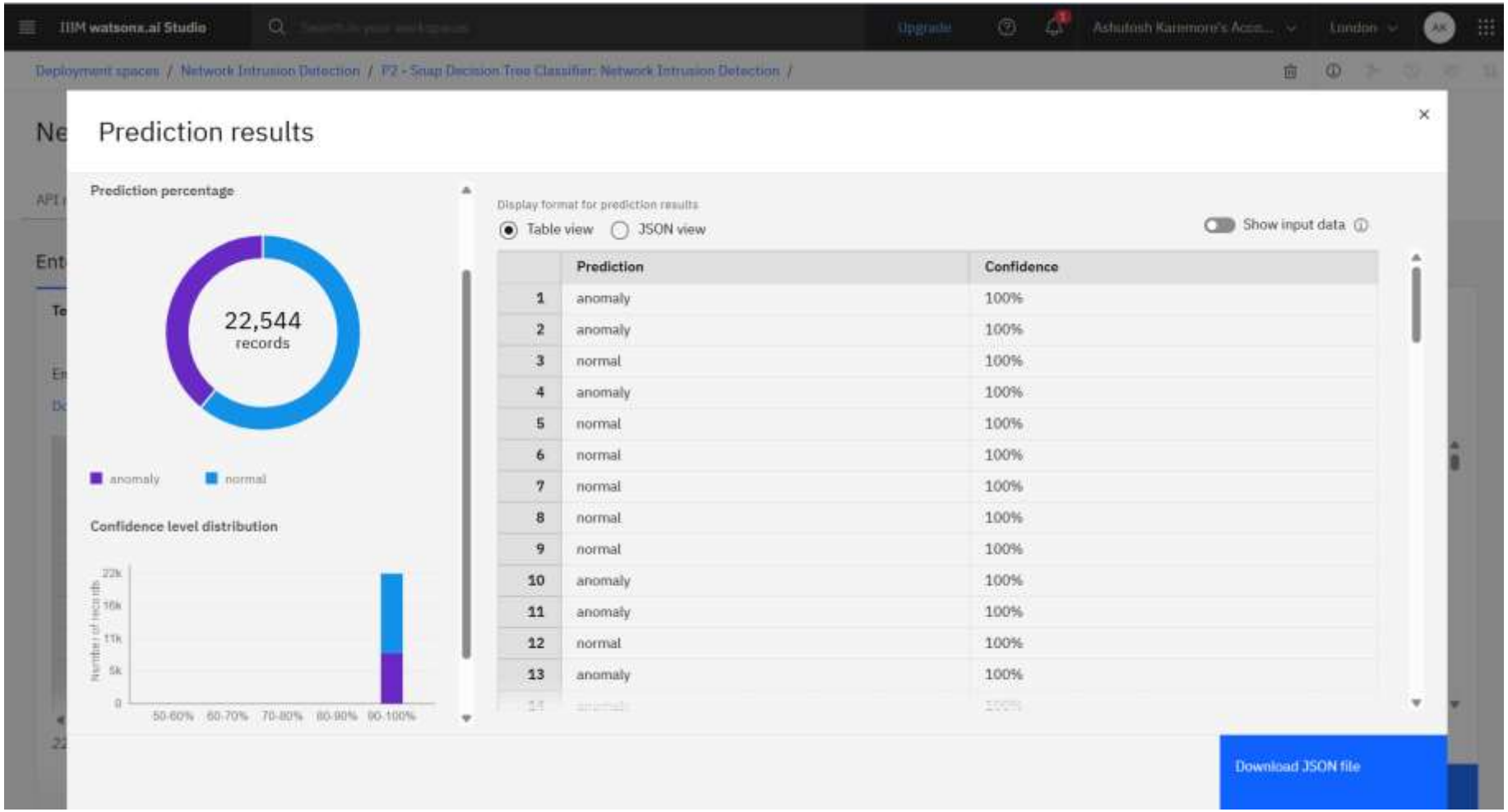
edunet foundation

RESULT



edunet foundation

RESULT



edunet foundation

CONCLUSION

- We have successfully trained a machine learning algorithm and created a model with predict the network intrusion activity with an accuracy of 99.5%.
- Detecting Network Intrusion is very crucial for timely rectifying any underlying issue that might affect business services, our model has learned and predicted with a high accuracy. Further with more real-time data we can learn our model to continuously adopt to the changing data.

FUTURE SCOPE

- Detecting Network Intrusion is very crucial for timely rectifying any underlying issue that might affect business services, our model has learned and predicted with a high accuracy. Further with more real-time data we can learn our model to continuously adopt to the changing data.

REFERENCES

- Decision Tree Classifier Paper : https://ieeexplore.ieee.org/document/6498972/
- https://www.sciencedirect.com/science/article/pii/S1877050916311127
- Dataset used: https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection
- https://cloud.ibm.com/docs
- https://www.ibm.com/docs/en/watsonx/saas?topic=solutions-autoai-machine-learning

IBM CERTIFICATIONS

edunet foundation

IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution

IBM

Shaik Afrin

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

Issued on: Jul 20, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/956ffaa9-08db-49c7-99b2-9a7c35ea2479

IBM

IBM CERTIFICATIONS

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Shaik Afrin

for the completion of

Lab: Retrieval Augmented Generation with LangChain

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

Completion date: 24 Jul 2025 (GMT) **Learning hours:** 20 mins

THANK YOU

edunet foundation